Banque et fichiers de clientèle informatisés

Poullet, Yves

Published in:
Revue de la Banque

Publication date:
1982

Document Version
le PDF de l'éditeur

III A. 70

Banque et fichiers de clientèle informatisés :

Principes de la règlementation juridique en Europe

Par Poullet Yves

Tournai 1952, Licencié en Droit (1974), Licencié en Philosophie (1977) U.C.L., Attaché au Centre-Informatique et Droit des Facultés de Namur.
Adresse : Rue du curé, 4 - 4271 Moxhe.

1 De nombreux pays d'Europe Occidentale réglementent l'utilisation de l'informatique. Ces législations (cfr. la liste reprise en annexe) cherchent à *équilibrer ou à concilier d'une part le "juste„ droit à l'information des entreprises ou administrations et d'autre part, la liberté et le droit à l'information des fichés.*
Nous développerons brièvement l'application de ce principe au secteur bancaire et dégagerons successivement les règles relatives à la constitution du fichier bancaire (n° 2 à 4), celles relatives à son fonctionnement (n° 5 à 8) et au contrôle de son fonctionnement (n° 9), celles enfin relatives au "droit à l'image„ que le fiché peut exercer face à la banque (n°10 à 16).

La constitution du fichier bancaire

2 La constitution d'une banque de données nominatives, ne peut en principe rester secrète (sauf en Allemagne).
L'organisme bancaire doit en *déclarer l'existence,* voire demander son autorisation (Luxembourg) auprès de l'organisme de contrôle (n° 9). Il mentionnera toute une série d'indications : noms et emplacement du système, son but, la nature et l'origine des données, les catégories d'invidus repris, les utilisateurs de ces données, etc...
L'organisme de contrôle reprendra partiellement ou complètement ces indications dans un registre tenu à la disposition du public (sorte de carte d'identité du système). Les modifications aux indications de base seront pareillement communiquées et publiées.

3 Lors de la constitution du fichier, la banque *nomme un responsable* à la protection des données. Ce responsable veillera au respect de la législation en vigueur et des divers codes déontologiques propres à la profession d'informaticien.

4 Enfin, des techniques de sécurité (Data Security) doivent être prises (exemple: installation d'un système de back-up). Elles seront fonction du caractère sensible, du volume et de la fréquence d'utilisation des données, des catégories et de la diversité des utilisateurs, et enfin de l'environnement du système de traitement des données (1).

(1) R. Turn, *Privacy Protection in Record Keeping Systems*, In and Management, 19.., 189. L'auteur résume ainsi les principes affirmés par la commission fédérale américaine.

Le fonctionnement du fichier bancaire

5 La première question touche bien évidemment du *contenu même du fichier bancaire*. La banque ne peut traiter que des données pertinentes, c'est à dire les données nécessaires à la bonne exécution de la relation contractuelle avec le fiché: la gestion d'un compte ou d'un crédit, par exemple.

Deux délibérations de la CNIL (Commission française de contrôle) citées en annexe, ont donné de ce principe une application précise. Ainsi, pour les fichiers relatifs à la gestion du crédit, seules peuvent être reprises:

«a Identité: nom, prénoms, adresse postale, date et lieu de naissance, numéro du dossier de prêt, identité bancaire;

b Situation familiale: s'il y a lieu, situation matrimoniale, état civil, situation professionnelle du conjoint;

c Logement: s'il y a lieu, caractéristiques du logement;

d Vie professionnelle: catégorie socio-professionnelle;

e Situation économique et financière: montant des ressources, caractéristiques du crédit, intérêts, commissions, assurances, garanties, montant des risques;

f Consommation de certains biens et services: notamment électro-ménager, automobile, voyages;

g Santé: éventuellement majoration de prime sur information de l'entreprise d'assurances.»

Des données sont a priori exclues: données relatives à l'appartenance raciale, politique, syndicale ou religieuse, données relatives à l'intimité de la vie privée. Certaines lois (danoise, canadienne, suédoise) interdisent la conservation de certaines données du passé judiciaire (faillite, chéques sans provision,...) au delà d'un certain temps (2).

(2)
... il s'agit d'un véritable "droit à l'oubli„. Le délai est généralement fonction de la gravité du délit (minimum cinq ans, maximum quatorze ans)

6 La collecte de ces données se fera par des moyens honnêtes, licites et loyaux. Elle s'opérera de préférence directement *auprès du fichier.* Le questionnaire mentionnera alors notamment le caractère obligatoire ou facultatif des réponses, les conséquences d'un défaut de réponse, etc... Lorsque les renseignements sont prix *auprès d'agences de renseignements commerciaux,* quelques lois (allemande, américaine, anglaise, suédoise) obligent la banque soit à demander l'autorisation au client, soit au moins à l'avertir de la prise de renseignements et de leur origine en cas de contestation quant à leur exactitude. Cet avertissement peut être fait par une simple inscription dans le formulaire de demande de crédit à condition qu'elle soit apparente et claire.

Enfin, de façon générale, les législations obligent à une mise à jour fréquente des données. Un logiciel permettant cette mise à jour fréquente est donc une nécesssité.

7 Le traitement de ces données, ajoute la loi française, ne peut être le seul fondement d'une décision à l'encontre du fiché. Il s'agit d'une condamnation explicite de la pratique du *"credit-scoring„.*

8 L'utilisation des données traitées doit être réservée aux seules personnes de la banque qui interviennent pour l'exécution de l'opération à la base du fichage (exemple: pour les données relatives au crédit, doivent seuls avoir accès le personnel chargé de la gestion du crédit et ses supérieurs hiérarchiques).

Ces données, brutes ou traitées, ne peuvent évidemment être cédées ou utilisées *en dehors de la banque,* sauf si cette transmission est nécessaire pour la bonne exécution de l'opération à la base du fichage ou dans la mesure où "cette transmission est nécessaire à la sauvegarde d'intérêts légitimes„ de la banque, d'un tiers ou de la collectivité. Ainsi, on peut estimer que des informations relatives à un crédit déterminé soient transmises à l'entreprise d'assurance-crédit concernée par l'opération, à la direction générale des impôts dans le cadre d'une enquête fiscale et à la caution.

Le contrôle du fonctionnement du fichier

9 Toutes les législations prévoient la nomination d'une *institution spécifique de contrôle des fichiers informatisés.* Cette institution opère d'office ou à la demande d'un fiché. Elle dispose des plus larges pouvoirs d'investigation et poursuit devant les autorités judiciaires les infractions dont elle a connaissance.

Le droit à l'image du fiché

10 Par fiché, la plupart des législations entendent la seule *personne physique* et non la *personne morale.* Sauf au Luxembourg, au Danemark et en Autriche, les fichiers relatifs aux personnes morales ne sont pas visées par les législations protectrices des données. Remarquons cependant que les personnes physiques pourront exercer leur "droit à l'image„ vis à vis de fichiers relatifs aux personnes morales pour autant que ces fichiers contiennent des données à leur propos. Ainsi, pour évaluer le crédit d'une société, la banque peut collecter des renseignements à propos des dirigeants de cette société. Ces dirigeants auront accès à ces renseignements.

11 Le *droit d'accès* de la personne fichée se définit comme son droit à "participer à la formation de l'image que les personnes qui l'entourent se font de lui„. Il s'agit non seulement de permettre à la personne concernée de connaître où elle est fichée et les données

reprises, éventuellement de les compléter ou de les rectifier, mais aussi de savoir pourquoi on l'interroge et de connaître globalement les réseaux d'informations qui l'entourent.
Ces deux derniers points ont déjà été évoqués: le fiché, lors de la collecte des renseignements, doit savoir pourquoi on l'interroge (N° 6). Par le registre public (n° 2), il peut connaître l'état de fichage de la société dans laquelle il vit.

12 Examinons maintenant les autres points. Le droit d'accès est d'abord le droit du fiché de *connaître l'existence d'informations le concernant dans un fichier.* On considère en général que le fiché par le fait même qu'il est en relation d'affaires avec la banque, peut et doit savoir que celle-ci traite des données à son sujet (système dit de la notification implicite). On n'oblige donc pas la banque à avertir systématiquement les clients du fait qu'ils sont fichés.

13 Le droit d'accès se comprend ensuite comme le droit du fiché de *connaître les informations le concernant,* présentes dans un fichier. En d'autres termes, le fiché peut demander à voir sa fiche. Il devra alors justifier de son identité (envoi de la copie d'une pièce d'identité). La demande aura lieu par écrit ou oralement à l'agence bancaire même. Le fiché peut se faire accompagner. La réponse bancaire sera faite dans les plus brefs délais (généralement prévus par la loi: un mois), par écrit ou oralement (éventuellement par téléphone, à condition de noter le contenu de la communication). Quant au coût de cette demande, il est fixé de façon forfaitaire par chaque loi (Allemagne: 10 DM, France: 20 NF). L'impact technique de cette forme du droit d'accès est important. Les ficheurs doivent pouvoir à tout moment sortir les données relatives à un fiché et décrire leurs utilisations depuis la dernière demande ou du moins dans les douze derniers mois.
La commission de contrôle suédoise en évalue le coût pour les entreprises à 25 % du coût global des diverses normes imposées par la loi de protection des données.

Enfin, notons que la loi française interdit aux ficheurs de maintenir dans leur fichiers l'information "utilisation du droit d'accès„ au delà de six mois.

14 Quelles sont les informations détenues qui doivent être communiquées au fiché? Les lois, en général, prévoient la *communication des informations de base* prises sur le fiché mais n'exigent pas en outre la délivrance des informations relatives à l'origine de ces informations (les sources), ni à la destination de ces informations (les tiers à qui transmission des informations est faite), ni au résultat du traitement (ex.; le "credit-scoring„ de la personne).

15 Le droit d'accès s'entend enfin du droit du fiché *à contester, rectifier ou compléter son image.* Un mot, tout d'abord de la procédure: quelques législations (projet belge et loi danoise) prévoient explicitement l'existence d'une *phase précontentieuse.* La banque a tout intérêt à demander à la personne responsable (n° 3) d'organiser un service d'accueil et de plainte des personnes fichées. L'échec de la phase précontentieuse oblige le fiché ou le ficheur à saisir la juridiction compétente. Cette juridiction sera la juridiction civile ou pénale normalement compétente et non une juridiction d'exception (sorte de tribunal de l'informatique). Le fiché, lors de ces procédures, peut se faire assister voire représenter par la commission dite de contrôle déjà évoquée (n° 9).

16 Si le droit de contester, de rectifier, de compléter une information est reconnu dans toutes les législations, on peut noter à ce propos quelques formules originales:

— Lorsque l'exactitude d'une information est contestée, la législation allemande prévoit sont blocage immédiat; le projet belge l'affecte d'un indice de doute. La loi américaine permet au fiché d'adjoindre à l'information une déclaration reprenant ses objections.

— Aucune législation n'autorise le fiché à ajouter des informations d'une nature différente

de celles déjà reprises. Par contre, le droit de compléter les informations est reconnu pratiquement dans toutes les législations (ex.: le fiché peut avoir intérêt à donner quelques précisions sur la catégorie socio-professionnelle à laquelle il appartient, en mentionnant les diplômes qui lui permettent des espoirs de carrière rapide).

— Enfin, certaines lois (Danemark, projet belge, Suède, Etats-Unis) octroient au fiché le "droit de suite„, c'est-à-dire le droit d'exiger du ficheur qu'il communique le complément ou la rectification d'information aux tiers qui ont utilisé ou utilisent ces données.

Annexe

Législations sur le plan international

— *OCDE,* Lignes directrices régissant la protection de la Vie Privée et les flux transfrontières de données de caractère personnel, 23 septembre 1980

— Conseil de l'Europe, Convention pour la protection des personnes à l'égard du traitement des données à caractère personnel, 21 janvier 1981.

Législations sur le plan national (en Europe)

— *Belgique:* Projet de loi provisoire assurant la protection de certains aspects de la vie privée.

— *Danemark:* Loi danoise n°293 sur les registres privés, 8 juin 1978.

— *France:* Loi n° 78-17 du 6 janvier 1978, Informatique, fichiers et libertés.

• CNIL, Délibération du 8 juillet 1980, concernant les traitements automatisés d'informations relatifs à la tenue des comptes de la clientèle et le traitement des informations s'y rattachant par les établissements bancaires, J.O. 19 août 1980.

• Délibération du 8 juillet 1980, concernant les traitements automatisés d'informations nominatives relatifs à la gestion des crédits ou des prêts consentis à des personnes physiques par les établissements bancaires et assimilés, J.O. 19 août 1980.

— *Luxembourg:* Loi du 31 mars réglementant l'utilisation des données nominatives dans les traitements informatiques.

— *Norvège:* Loi du 9 juin 1978 sur les registres de personnes.
— *République fédérale d'Allemagne:*
Bundesdatenschutzgesetz, 27 janvier 1977
— Royaume-Uni: Consumer Credit Act, 1974
— *Suède:*
Data Act, 11 mai 1973 (amendée le 1 juillet 1979)
Fair Credit Reporting Act, 14 décembre 1973

Bibliographie

- *Inria,* Etude sur la confidentialité et la sécurité des données, Rapport final à la Commission des Communautés
Européennes, 2 vol.
- *Banques de données, entreprises-vie privée,* Actes du Colloque tenu à Namur les 25 et 26 septembre 1979, Creadif, Bruxelles.

Banque et services informatisés à la clientele:
l'Electronic Fund Transfer Act américain
(E.F.T. Act 15 USC § 1693 (1978))

17 Les banques américaines, dans un premier temps, européennes dans un second temps, mettent à la disposition de leur clientèle des services informatisés notamment pour le dépôt et le retrait de fonds, mais aussi pour le paiement de biens ou de services à des institutions tierces (grands magasins, pompes à essences, etc...) Ils est dès lors intéressant de donner quelques indications sur la réglementation américaine (aucune réglementation n'existe encore chez nous en Europe (3)) de ces services informatisés bancaires.

18 La loi américaine rassemble ces divers services informatisés bancaires sous la dénomination de "transfert électronique de fonds„. Elle définit cette notion comme suit: "Tout transfert effectué par un terminal informatique, téléphone ou computer ou magnetic tape, autre que celui qui est fondé par un support papier (sauf exception) et qui ordonne ou autorise une institution financière à débiter ou créditer un compte client. Sont notamment visés: les transferts à partir de point de vente, les

(3)
On notera que la jurisprudence française (Angers 2 déc. 1980, D. 1981, I.R., 353, obs. M. Vasseur; Banque, 1981, 511, obs. L.M. Martin; Lyon 9 juillet 1981, G.P., 1981, 2, 20-21 nov., p. 9) estime que l'abus de distributeur de billets par le titulaire d'un compte non provisionné ne peut être pénalement incriminé.

opérations à partir de machines conversationnelles automatisées (automated teller machine); dépôts directs ou virements de fonds et transfert par téléphone.

19 La mise à la disposition du public de ces services informatisés entraîne à charge de la banque des obligations générales et des obligations spécifiques.

Les obligations générales sont les suivantes:
a En aucune façon, elle ne peut faire de l'emploi du service informatique, une condition à l'octroi d'un crédit supplémentaire.
b Elle doit révéler au client les termes et conditions de l'utilisation du service et elle doit l'informer de ses droits et responsabilités en *langage compréhensible*. Elle ne doit délivrer la clef d'accès que dans la mesure où il y a demande écrite (sauf si la clef remplace un système déjà accepté).
c Si une modification dans le mode d'emploi du service informatique s'avère nécessaire, elle préviendra chaque client au moins deux jours à l'avance.
d En aucune manière, elle ne peut interrompre les différents services informatisés rendus au client sauf si les fonds de ce dernier sont insuffisants, si l'opération que le client désire effectuer sort des limites de son crédit, sauf enfin si un procès légal oppose la banque au client.

En dehors de ces cas, la responsabilité de l'interruption du service incombe à la banque (4). Celle-ci pourra s'exonérer en démontrant que l'arrêt résulte de circonstances hors de son contrôle et ne pouvait être prévenu malgré des efforts raisonnables et diligents (ex.: acte de terrorisme) ou que l'arrêt provient d'un disfonctionnement technique dont le client était averti.

20 La loi américaine prévoit en outre des obligations spécifiques à chaque type d'opération informatisée. On distingue ainsi:
a *Les opérations à partir de terminaux:*

(4) Comp. la décision française (Provost Masurel c. Crédit Lyonnais, Trib. comm. Roubaix 2 juillet. 1980, D. 1980, 518, note Y. Le Tartre): "En règle générale, les billets à vue sont présentés dans un délais maximum de dix jours après leur remise et l'emploi d'un système informatique ne saurait justifier un délai plus long puisque il doit, en principe accélérer les relations commerciales„.

Chaque opération doit donner lieu à l'émission d'un reçu qui reprend :

— le montant et la date de l'opération,
— le type de transfert,
— l'identification du compte,
— le lieu ou l'identification du terminal,
— l'identité des tiers visés par l'opération.

b *L'ordre permanent de crédit émanant de tiers :* au départ, la loi imposait à la banque d'avertir le client si l'ordre de crédit (par exemple le paiement du salaire par l'employeur) était ou non effectué. Très vite, la commission de contrôle américaine (n°9) jugea que la banque pouvait se contenter de renseigner au client un numéro de téléphone où ce dernier pourrait à tout moment connaître sa situation.

c *L'ordre permanent de paiement émanant du client.*
Une autorisation écrite du client est nécessaire pour ce type d'opérations. Il doit être possible pour le client d'interrompre l'ordre permanent à tout moment et par tous moyens. L'institution de crédit pourra évidemment exiger une confirmation écrite de cette interruption.
Enfin, la banque doit remettre à ses clients au moins tous les mois un document (le "Periodic Statement„) reprenant :

- numéro de téléphone et adresse pour réclamation en cas d'erreur,
- montant du compte au début et à la fin du mois,
- intérêts créditeurs ou débiteurs de la période,
- diverses opérations effectuées sur le compte pendant la période avec leur identification

21 Un des problèmes les plus importants posés par l'utilisation des services informatiques est certes la question de l'erreur (exemple : un paiement est fait à une personne qui n'y avait pas droit). La loi américaine prévoit une procédure particulière pour la solution de cette question : premièrement, le client doit notifier par oral ou par écrit l'erreur dans les soixante jours de l'envoi du "periodic statement„ ; en outre, il

donnera à la banque des informations complémentaires permettant l'identification du nom du client, du numéro du compte, du montant de l'erreur et des raisons du client de croire à l'erreur. La banque enquêtera. Elle est tenue d'envoyer dans les dix jours les résultats. Si dix jours se révèlent insuffisants, la banque pourra éventuellement étendre le délai à 45 jours. Dans l'attente, elle devra recréditer le compte du client du montant contesté et laisser à ce dernier le plein usage de la somme. Après ce délai, ou bien elle estime qu'il y a erreur de sa part et elle recrédite définitivement alors le compte du montant contesté, ou bien elle estime qu'il n'y pas d'erreur, et elle se doit alors d'expliquer les raisons de son refus de maintenir le crédit.
A la demande du client, elle donnera toute la documentation possible. Il est évident que le client peut refuser de se plier à la décision bancaire. Il porte alors l'affaire au tribunal civil. C'est *à la banque,* et non *au client* qu'il appartiendra de faire la preuve qu'il n'y a pas eu d'erreur. Si la responsabilité du banquier en cas d'erreur de sa part n'est pas limitée, celle du client sera, de toute façon, limitée à 50 $ en général, à 500 $ si le client a omis de réclamer dans le délai prescrit ou s'il a omis de déclarer le vol ou la perte de la "clef„ qui lui permettait l'accès au service bancaire.